INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR2004/001362

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/08 H04L9/30

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, PAJ, WPI Data, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
T	BILLET O, GILBERT H: "A Traceable Block Cipher" ASIACRYPT 2003: 9TH INTERNATIONAL CONFERENCE ON THE THEORY AND APPLICATION OF CRYPTOLOGY AND INFORMATION SECURITY (SPRINGER-VERLAG, HEIDELBERG, LECTURE NOTES IN COMPUTER SCIENCE 2894), November 2003 (2003-11), pages 331-346, XP002273113 ISBN: 3-540-20592-6 the whole document	1-15

-/--

[X] Further documents are listed in the continuation of box C.

[ ] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10 August 2005	24/08/2005

Name and mailing address of the ISA
European Patent Office, P.B. 5818 Patentlaan 2
NL – 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax (+31-70) 340-3016

Authorized officer

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR2004/001362

C(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	BONEH D ; FRANKLIN M: "An efficient public key traitor tracing scheme" ADVANCES IN CRYPTOLOGY - CRYPTO'99. 19TH ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE. PROCEEDINGS, 19 August 1999 (1999-08-19), pages 338-353, XP002273114 Santa Barbara, CA, USA ISBN: 3-540-66347-9 page 338 - page 343	1,2
A	MATSUMOTO T; IMAI H: "PUBLIC QUADRATIC POLYNOMIAL-TUPLES FOR EFFICIENT SIGNATURE-VERIFICATION AND MESSAGE-ENCRYPTION" ADVANCES IN CRYPTOLOGY- EUROCRYPT '88. INTERNATIONAL CONFERENCE ON THE THEORY AND APPLICATION OF CRYPTOGRAPHIC TECHNIQUES, PROCEEDINGS. SPRINGER VERLAG, DE, 1988, pages 419-453, XP000568374 ISBN: 3-540-50251-3 cited in the application the whole document	3-15
A	MENEZES; OORSCHOT; VANSTONE: "HANDBOOK OF APPLIED CRYPTOGRAPHY, PASSAGE" CRC PRESS SERIES ON DISCRETE MATHEMATICS AND ITS APPLICATIONS, 1997, pages 551-552, XP002273115 BOCA RATON, FL, USA ISBN: 0-8493-8523-7 page 551, paragraph 13.3.1 - page 552	1,2
A	PATARIN J ; GOUBIN L ; COURTOIS N: "Improved algorithms for isomorphisms of polynomials" ADVANCES IN CRYPTOLOGY - EUROCRYPT '98. INTERNATIONAL CONFERENCE ON THE THEORY AND APPLICATION OF CRYPTOGRAPHIC TECHNIQUES. PROCEEDINGS, 4 June 1998 (1998-06-04), pages 184-200, XP002273116 Espoo, Finland ISBN: 3-540-64518-7 the whole document	3-15